

Notice of Allowability

Application No.

09/726,433

Examiner

Samson B. Lemma

Applicant(s)

KUROIWA ET AL.

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to RCE is filed on 06/09/2005.
2. ☒ The allowed claim(s) is/are 1-7,15,16 and 18.
3. ☒ The drawings filed on 14 March 2003 are accepted by the Examiner.
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) ☐ All b) ☐ Some* c) ☐ None of the:
 1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
 6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
 - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08),
Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit
of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413),
Paper No./Mail Date _____
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____

DETAILED ACTION

1. The request filed June 9, 2005 for a request for continued examination (RCE) under 37 CFR 1.114 based on patent application 09/726433 is acceptable and an RCE has been established. Accordingly, claims 1-7; 15-16 and claim 18 have been examined.
2. Claims 8-14; 17 and 19-22 have been cancelled.
3. Claims 1-6; 15-16 have been amended.
4. No new claims have been added.

Allowable Subject Matter

5. Claims 1-7; 15-16 and 18 are allowed.
6. The following is an examiner's statement of reasons for allowance:
7. With respect to the independent claims 1-6 & 15 the art on the record, namely the combination of Eyer and Funakoshi discloses most of the limitation of the recited claims 1-6. Furthermore Funakoshi discloses how, an authentication key which is interpreted to be the second key by the office, can be generated on the first unit on the basis of initial-value or the seed generated at the first unit according to a predetermined key generation algorithm and transmitting the initial-value information or the seed to the second- unit and this second unit receives the seed through its seed receiving portion and by identifying the predetermined key

generation algorithm, the second unit generates a key from the initial-value information or the seed by encoding this initial value or seed which has been received from the first-unit and eventually producing the same key which is the same as the authentication key which had been generated at the first unit. (column 2, lines 59-67; column 3, lines 1-22).

However, the art on the record namely the combination of Eyer and Funakoshi does not disclose or suggest the following particular limitation of the respective claims 1-6 and claim 15 "wherein it is previously decided that the plurality of predetermined key generation algorithms are usable by a decrypting device in decryption of the encryption-resultant contents information, and the algorithm identification information is for identifying the one among the plurality of predetermined key generation algorithms which should be used by the decrypting device in response to a reference table holding the plurality of predetermined key generation algorithms."

None of the prior art of record taken singularly or in combination teaches or suggests a method/apparatus/transmission or recording medium/ of transmitting information with all the limitations recited in respective claims in combination with the following functional limitation "wherein it is previously decided that the plurality of predetermined key generation algorithms are usable by a decrypting device in decryption of the encryption-resultant contents information, and the

algorithm identification information is for identifying the one among the plurality of predetermined key generation algorithms which should be used by the decrypting device in response to a reference table holding the plurality of predetermined key generation algorithms ."

For the reasons provided above, the amended independent claims 1-6 & 15 are allowed.

8. With respect to the independent claim 16 the art on the record, namely the combination of Eyer and Funakoshi discloses most of the limitation of the recited claim 16. However, the art on the record namely the combination of Eyer and Funakoshi does not disclose or suggest the following particular limitation of the respective claim 16, "a reference table storing the plurality of predetermined key generation algorithms identifiable by algorithm identification information, wherein it is previously decided that the plurality of predetermined key generation algorithms are usable by a decrypting device in decryption of the encryption-resultant contents information."

None of the prior art of record taken singularly or in combination teaches or suggests a method of decryption information with all the limitations recited in respective claim 16 in combination with the above underlined functional limitation.

For the reasons mentioned above, the amended independent claims 16 is also allowed.

Art Unit: 2132

9. The dependent claims 7 & 18, being further limiting to the independent claims, definite and enabled by the specification are also allowed.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submission should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on. The fax phone number for the organization where this application or proceeding is assigned is 571-272-3799.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information


Art Unit: 2132

about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SAMSON LEMMA

S.L.

06/22/2005


GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100